Cassandra Crossing/ Il Cloud e me

(212)— Leggere attentamente le avvertenze e il foglio illustrativo. Può avere effetti collaterali. Non somministrare ai regimi nemici di…

Cassandra Crossing/ Il Cloud e me

(212)— Leggere attentamente le avvertenze e il foglio illustrativo. Può avere effetti collaterali. Non somministrare ai regimi nemici di Internet.

18 febbraio 2011—Nella precedente release di questa rubrica, Cassandra si è occupata di alcuni aspetti tecnici ed economici del **Cloud Computing** per le aziende: le conclusioni raggiunte consistevano in una serie di domande sull'impatto del cloud sulla Rete come la conosciamo oggi.

Per Cassandra ovviamente l'aspetto più interessante (diciamo così) del cloud è l'impatto sulla vita delle persone, particolarmente dal punto di vista della privacy, dei diritti digitali e del tecnocontrollo sociale.

Dal punto di vista della privacy il problema più importante, dato lo scambio di dati personali e potenzialmente sensibili con il fornitore di cloud, è se questo dati sono da lui conoscibili ed in caso positivo se sono utilizzati in qualche modo. Facciamo il caso più semplice di un fornitore di storage online, come Ubuntu One, o l'ormai defunto Ovi Storage di Nokia.

Il modo migliore per garantire la non conoscibilità dei dati è che questi siano crittografati prima di essere inviati allo storage online. L'operazione di crittografia deve essere eseguita dal client, e di questo dovrebbe essere data garanzia, sia contrattuale che tramite la fornitura del codice sorgente aperto del client stesso.

Sarebbe concettualmente possibile anche far viaggiare i dati in chiaro dal client al server e lasciare invece al server il compito di crittografare prima di memorizzare i dati su disco, ma anche in questo caso servirebbero le stesse garanzie del caso precedente, sia tecniche che contrattuali.

Purtroppo per la mia esperienza di cloud storage per utenti privati non ci sono servizi che offrano ambedue queste garanzie; anzi a voler essere precisi quasi tutti non ne offrono nessuna.

Quello che viene evidenziato dalle comunicazioni pubblicitarie è l'uso di protocolli criptati (SSL) per la trasmissione non intercettabile dei dati. Quest'ultima caratteristica è quello che può essere definito in modo colorito *'nu pannicello caldo*, anzi quasi una presa in giro perché chi meglio del fornitore del servizio è in grado di intercettare i dati inviati allo storage cloud?

Considerando che il caso del cloud storage è il più semplice tra tutti i servizi consumer che possono essere erogati da un cloud, è facile estrapolare queste caratteristiche di implementazione minimale e trascurata del servizio, che inevitabilmente conduce a rendere un cattivo servizio al consumatore di servizi cloud.

Come concetto accessorio di questo aspetto potremmo dare un giudizio abbastanza negativo sull'affidabilità del cloud storage per i consumatori. Infatti il primo esempio di fornitore di un cloud storage per privati che chiude il servizio e lascia in braghe di tela i suoi clienti c'è già stato, ed è il già ricordato Ovi Storage, che ha di punto in bianco annunciato la chiusura del servizio, preannunciandolo per fortuna con un certo anticipo in modo da permettere agli ex-clienti di ricopiarsi indietro i dati sul PC.

Si dirà che questa è una caratteristica innata non dei servizi cloud, ma dei servizi gratuiti, che bisogna accettarne il rischio e che certo gli stessi servizi in versione "professional" ed a pagamento sarebbero migliori.

Personalmente non ne sono troppo convinto: la contrattualistica dei servizi a pagamento (ed eccoci di nuovo a livello aziendale) è quasi sempre difensiva nei confronti del fornitore, spesso sotto un manto di legalese stretto.

Per quanto riguarda l'utilizzo dei dati conoscibili dal fornitore di storage possiamo fare l'esempio di Gmail, che dando uno spazio per i messaggi di posta dell'utente dichiara onestamente che li utilizzerà per i suoi scopi, persino nel caso di loro cancellazione.

E' senz'altro un caso "degenere" di cloud storage, ma il trend sembra chiaro. Se lo fa Google, che non è *evil*, cosa possono fare quelli che *evil* un po' (anzi parecchio) lo sono?

E quindi cosa dire della privacy degli utenti del cloud storage? Che viene implicitamente garantita dai messaggi pubblicitari e promozionali, ma che in realtà solo i contratti commerciali offrono (quasi sempre) reali garanzie legali di non utilizzo dei dati inviati al cloud. Si tratta di garanzie legali perché non mi

risulta che garanzie tecniche, quali appunto l'**ispezionabilità** del codice della componente client del cloud, siano offerte da nessun provider di cloud storage.

E veniamo agli aspetti legati ai diritti digitali.Molti music store, agendo come fornitori di servizi cloud, offrono la possibilità di comprare musica mantenendo i relativi file nel cloud e permettendone la fruizione via streaming ovviamente sotto la "protezione" di opportuni DRM.

Da un punto di vista legale si tratta sostanzialmente di un "accordo di licenza" sul servizio e sopratutto sui contenuti acquistati. E' anche una rinuncia alla fonte della possibilità di esercitare il diritto di primo acquisto, che garantisce la possibilità di rivendere la musica acquistata, come quando si rivende un CD usato su Amazon o su una bancarella del mercato.

Anche qui si tratta di un "piccolo" diritto digitale a livello di consumatore, ma l'approccio stesso di un contratto tra un fornitore forte e un contraente debole porta a dubitare che servizi non vantaggiosi al massimo per il fornitore verranno mai venduti.

E la speranza che una sana concorrenza permetta questo atteggiamento virtuoso viene meno appena si ricorda quanto spesso si siano creati "cartelli" di fornitori che offrivano caratteristiche omogenee per non farsi concorrenza, e mettere quindi in posizione di svantaggio e di debolezza tutti i loro clienti.

Ed infine facciamo qualche considerazione sulle possibilità di maggior controllo sociale introdotta da un uso diffuso di servizi cloud. Qui il discorso si fa assai più complesso, e meriterebbe una puntata a parte.

Sorvolando sulle possibilità di intercettazione e memorizzazione di dati personali che ad esempio il cloud storage offrirebbe (vedi il caso dei dati di cella delle reti GSM), basta pensare alle opportunità di "staccare la spina" o di minacciare di farlo come strumento di potere. I recenti fatti egiziani insegnano quanto potere sia in mano a chi, come una stato, può mettere in atto un vero e proprio "attacco DoS" di negazione di servizio contro i propri cittadini.

Quanto più il cittadino dipende da servizi erogati da terzi, e quindi da aziende, tanto più si amplia lo spazio in cui uno stato può imporre ad essi la negazione di un servizio e quindi esercitare un potere ancora maggiore sui suoi cittadini, sempre meno cittadini e sempre piùsudditi.

Per concludere, a Cassandra preme sottolineare che queste considerazioni sono applicabili già ad un semplice servizio come quello di cloud storage.

Quanto si amplificano se si considerano servizi più critici ed indispensabili, come appunto la connettività alla Rete, la disponibilità dei servizi medici o bancari online, ed altri che vengono lasciati come esercizio al lettore?

Forse si dovrebbe concludere sintetizzando tutto in uno slogan: "Cloud, se lo conosci lo eviti".

Originally published at punto-informatico.it.

Nota per che riceve gli articoli via mail. *Medium.com modifica automaticamente i link contenuti negli articoli quando li invia per mail, rendendoli traccianti.* ***La cosa disgusta Cassandra****, che se ne è accorta solo di recente grazie ad una provvidenziale segnalazione. Se ciò superasse il vostro limite di indignazione, ed in attesa che Cassandra trovi una soluzione od un'alternativa, potete fruire dell'articolo direttamente sul sito.*

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on May 12, 2023.

Canonical link

Exported from Medium on January 2, 2024.